Course code	Course Name	L-T-P - Credits	Year of Introduction
IT402	Cryptography & Cyber Security	3-0-0-3	2016

Prerequisite: CS201 Discrete computational structures

Course Objectives

- To understand the mathematics behind Cryptography.
- To understand the security concerns and vulnerabilities
- To familiarize with different types of cryptosystems
- To create an awareness for the design of various cryptographic primitives
- To analyze different types of attacks on various cryptosystems.

Syllabus

Basics of Algebra and number theory – Security goals, services and mechanisms – cryptography-traditional and modern secret key ciphers –data encryption standard – advanced encryption standard –public key crypto systems- digital signature – IP security

Expected outcome .

The students will be able

- To learn the importance of number theory in designing crypto systems;
- To design public and private key cryptosystems;
- To do cryptanalysis of various cryptosystems.

Text Books:

1. Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography & Network Security, Second Edition, Tata McGraw Hill, New Delhi, 2010
2. Douglas R. Stinson, "Cryptography: Theory and Practice", Third Edition, CRC Press.
3. William Stallings, "Cryptography and Network Security – Principles and Practices", Pearson Education, Fourth Edition, 2006.

References:

1. Atul Kahate, "Cryptography and Network Security", 2nd Edition, Tata McGraw Hill, 2003.
2. Bernard Menezes, Network Security and Cryptography-Cengage Learning India, 2011
3. Bruce Schneier, "Applied Cryptography: Protocols, Algorthms, and Source Code in C", Second Edition, John Wiley and Sons Inc, 2001.
4. Thomas Mowbray, "Cybersecurity : Managing Systems Conducting Testing, and Investigating Intrusions", John Wiley, 2013
5. Wenbo Mao, " Modern Cryptography- Theory & Practice", Pearson Education, 2006.

Course Plan

Module	Contents	Hours	Sem. Exam Marks
I	**Basics of Algebra and Number Theory**: Integer Arithmetic- Modular Arithmetic- Algebraic structures – Prime Numbers - Fermat's and Euler's Theorem – Factorization - Chinese Remainder Theorem - Linear and Quadratic Congruence - Discrete Logarithms.	7	15%
II	Introduction to Security:-Security Goals – Security services (Confidentiality, Integrity, Authentication, Non-repudiation, Access control) – Security Mechanisms (Encipherment, Data Integrity, Digital Signature, Authentication Exchange, Traffic Padding, Routing Control, Notarization, Access control) -	7	15%

	Security Principles. Introduction to Cryptography:- Kerckhoff's Principle -Classification of Cryptosystems- Cryptanalytic attacks- Cipher Properties (Confusion, Diffusion).		
FIRST INTERNAL EXAMINATION			
III	Traditional Secret Key Ciphers:- Substitution Ciphers (mono alphabetic ciphers, poly alphabetic ciphers)-Transposition Ciphers-Stream and Block Ciphers. Modern Secret Key Ciphers:- Substitution Box-Permutation Box-Product Ciphers	7	15%
IV	Data Encryption Standard (DES) (Fiestel and Non-Fiestel Ciphers, Structure of DES, DES Attacks, 2-DES, 3-DES) - Advanced Encryption Standard (AES) (Structure, Analysis)- Cryptographic Hash Functions– Properties - Secure Hash Algorithm-Message Authentication Code (MAC).	7	15%
SECOND INTERNAL EXAMINATION			
V	Public Key Cryptosystems (PKC): - Types of PKC –Trapdoor - one way functions -RSA Cryptosystem (Integer Factorisation Trapdoor**,** Key Generation, Encryption, Decryption) - El Gamal Cryptosystem (Discrete Logarithm Trapdoor**,** Key Generation, Encryption, Decryption) - Diffie-Hellman Key Exchange Protocol, Man in the Middle attack on Diffie-Hellman Protocol.	7	20%
VI	Digital Signature:-Signing – Verification - Digital signature forgery (Existential forgery, Selective forgery, Universal forgery) - RSA Digital Signature Scheme - ElGamal Signature Scheme - IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload-Intruders, Intrusion Detection, Distributed Denial of Service attacks	7	20%
END SEMESTER EXAM			

QUESTION PAPER PATTERN

Maximum Marks: 100 Exam Duration: 3 hours

The question paper shall consist of Part A, Part B and Part C.

Part A shall consist of three questions of 15 marks each uniformly covering Modules I and II. The student has to answer any two questions (15×2=30 marks).

Part B shall consist of three questions of 15 marks each uniformly covering Modules III and IV. The student has to answer any two questions (15×2=30 marks).

Part C shall consist of three questions of 20 marks each uniformly covering Modules V and VI. The student has to answer any two questions (20×2=40 marks).

Note : Each question can have a maximum of 4 subparts, if needed